What is claimed is:

1. A gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises:

a computing device comprising:

a monitoring process that monitors network traffic through the gateway;

a communication process that can communicate statistics collected in the gateway from the monitoring process with a control center and that can receive queries or instructions from the control center; and

a filtering process to allow filters to be inserted to filter out packets that the gateway deems to be part of an attack.

2. The gateway of claim 1 wherein the communication process couples to a dedicated link to communicate with the control center over a hardened network.

3. The gateway of claim 1 wherein the monitoring process in the gateway samples network packet flow in the network.

4. The gateway of claim 1 wherein the gateway is adaptable to be physically deployed in line in the network.

5. The gateway of claim 1 wherein, the gateway is adaptable to dynamically install filters on nearby routers.

6. The gateway of claim 1 wherein the monitoring process detects IP traffic and determines levels of unusual amounts

of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

7. The gateway of claim 1 wherein the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

8. The gateway of claim 1 wherein monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports.

9. The gateway of claim 1 wherein monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

10. The gateway of claim 1 wherein monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection.

11. The gateway of claim 1 wherein monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail.

12. The gateway of claim 11 wherein monitoring process maintains statistics on parameters including source and destination host or network addresses, protocols, types of

packets, number of open connections or of packets sent in either direction.

13. The gateway of claim 12 wherein monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold.

14. The gateway of claim 13 wherein monitoring process logs packets.

15. The gateway of claim 14 wherein monitoring process logs specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

16. A method of protecting a victim site during a denial of service attack, comprises:

disposing a gateway device between the victim site and a network;

monitoring network traffic through the gateway and measuring heuristics of the network traffic;

communicating statistics collected in the gateway to a control center; and

filtering out packets that the gateway or control center deems to be part of an attack.

17. The method of claim 16 wherein communicating occurs over a dedicated link to the control center via a hardened network.

18. The method of claim 16 wherein monitoring samples network packet flow in the network.

19. The method of claim 16 wherein the gateway is physically deployed in line in the network.

20. The method of claim 16 wherein filtering further comprises:

dynamically installing filters on nearby routers via an out of band connection.

21. The method of claim 16 wherein monitoring further comprises:

detecting IP traffic and determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

22. The method of claim 16 wherein monitoring further comprises:

detecting Internet Protocol (IP) traffic and determining levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

23. The method of claim 16 wherein monitoring further comprises:

detecting Internet Protocol (IP) traffic and determining levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

24. The method of claim 16 wherein monitoring further comprises:

detecting IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

25. The method of claim 16 wherein monitoring further comprises:

detecting a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

26. The method of claim 16 wherein monitoring further comprises:

logging statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

27. The method of claim 16 wherein monitoring further comprises:

issuing a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

28. The method of claim 16 wherein monitoring further comprises:

logging specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

29. A computer program product residing on a computer readable medium for protecting a victim site during a denial of service attack, comprises instructions for causing a computer device coupled at an entry to the site to:

monitor network traffic sent to the victim site and measuring heuristics of the network traffic;

communicate statistics collected in the computer device to a control center; and

filter out packets that the device or control center deems to be part of an attack.

30. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

sample network traffic flow.

31. The computer program product of claim 29 wherein instructions to filter further comprise instructions to:

dynamically install filters on nearby routers via an out of band connection.

32. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect IP traffic; and

determine levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

33. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect Internet Protocol (IP) traffic; and

determine levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

34. The computer program product of claim 29 wherein instructions to monitor further comprise instructions to:

detect Internet Protocol (IP) traffic; and

determine levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

35. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

detect IP traffic; and

determine levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

36. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

detect a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

37. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

log statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

38. The computer program product of claim 29 wherein instructions to monitor further comprises instructions to:

issue a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

39. The computer program of claim 29 further comprising instructions to cause the processor to receive communications from a control center to deliver data pertaining to the types of traffic passing through the gateway.